REMARKS/ARGUMENTS

I. Introduction:

Claims 1, 3, 8, 15, and 18 are amended, claims 2, 5, and 22 are canceled, and new claims 23-36 are added herein. With entry of this amendment, claims 1, 3-4, 6-21, and 23-36 will be pending.

II. Claim Rejections Under 35 U.S.C. 112:

Claim 2, which was rejected under 35 U.S.C. 112, has been canceled.

III. Claim Rejections Under 35 U.S.C. 103:

Claims 1, 3-6, 8-10, and 12-13 stand rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,598,034 (Kloth) in view of "Router Plugins: A Software Architecture for Next Generation Routers" (Decasper et al.).

Claim 1 is directed to a method for generating filters based on data entering a network device. The method includes: classifying network flow based on one or more packets received at the network device, performing a lookup based on the classified network flow and building a new flow cache entry if the lookup is unsuccessful; sending each of said network flows to a corresponding flow cache and implementing policies designated for each of said network flows; creating an aggregate network flow summary for each of said network flows; analyzing at least one of said aggregate network flow summaries to detect characteristics of potentially harmful network flows; and generating a filter to prevent packets corresponding to detected potentially harmful network flows from passing through the network device. Claim 1 has been amended to include

classifying network flows, performing a lookup, and creating an aggregate network flow summary.

Kloth discloses rule based IP data processing. The system processes lookups (i.e., destination port comprising forwarding information and packet processing action) in parallel. The system also allows any action to be applied to any packet based upon any rule that a network administrator may define. A packet is processed in one or two stages. At the first stage some packets may be routed directly without further processing. Otherwise the packet is classified and a route lookup is performed in parallel with the lookup of the rest of the attributes of the packet. Actions can be performed upon an IP flow or individual packets. Data flow or packets can be dropped intermittently or discarded altogether, as a result of a detected data pattern.

The Decasper et al. article describes a router software architecture which allows plugins to be dynamically added and configured at run time. One or more flows are bound to a specific plugin and each filter is associated with a pointer to a plugin instance. Data packets are passed to instances of plugins which implement specific functions for processing the packets. Data path mechanisms are applied to every single packet rather than a sample of packets within a network flow.

Applicant respectfully submits that claim 1 is not obvious in view of Kloth and Decasper et al. Neither of these references show or suggest an aggregate network flow summary created for network flows, analyzing aggregate network flow summaries to detect characteristics of potentially harmful network flows, and filters generated based on detected harmful flows. As discussed above, Kloth processes lookups in parallel and does not perform classification to separate network flows. Decasper et al. do not create aggregate network flow summaries which are analyzed and used to generate filters, as required by claim 1. Instead, Decasper et al. uses every single packet for data path mechanisms. Furthermore, rather than generating a filter to prevent harmful data from passing through a network device, Decasper et al. simply uses filters to specify flows

and corresponding plugins. Kloth also does not use aggregate flow summaries to detect characteristics of potentially harmful network flows and generate filters based on the analyzed flow, as set forth in claim 1. Kloth uses a set of rules to define a pattern to be compared in the incoming data flow, rather than analyzing an aggregate flow summary created from the network flows and generating filters based on the analyzed flow summaries.

Applicant's invention is particularly advantageous in that flow collection aggregation allows for data to be stored by aggregate summary records instead of raw data records. Furthermore, since each packet in the network flow is processed responsive to the entry for the network flow in the flow cache, the netflow mechanism is able to implement administrative policies which are designated for each network flow rather than for each packet. Network flows are thus analyzed and information on incoming packets can be provided without examining each packet received.

Moreover, Applicant respectfully submits that there is no suggestion to combine the teachings of Kloth with Decasper et al. to produce the claimed invention. Obviousness cannot be established by combining the teachings of the prior art to produce the claimed invention, absent some teaching, suggestion, or incentive supporting the combination. An important aspect of the Kloth invention is that different lookups are performed in parallel and that the packet is classified, if classification is required, only one time (see, for example, col. 3, lines 41-49, and col. 3, line 62 to col. 4, line13). The system classifies packets as early as possible with as much information as possible applied to every packet. Rather than performing classification sequentially, it performs it in full for the entire IP flow as early as possible in the process. The system of Kloth performs tasks in parallel to reduce latency. If Kloth were modified to classify packets into different network flows and apply policies at a later stage as performed by Decasper et al., a primary function of the Kloth system would be defeated. The law is clear that it would not be obvious to make a modification in such instances.

Accordingly, claim 1 is submitted as nonobvious over Kloth and Decasper et al.

Claims 3-4, 6-14, and 23-27, depending either directly or indirectly from claim 1, are submitted as patentable for the reasons discussed above with respect to claim 1.

Claim 8 is further submitted as patentable over Kloth and Decasper et al., which do not show or suggest hardware sending network flow to a corresponding flow cache and software performing network flow analysis.

New claim 24 provides for further refinement of the filter. Thus, once a group of packets are identified as harmful, the corresponding network flows can be analyzed to further refine the filter. Instead of filtering out all data arriving from an identified organization, only destructive packets received from an actual attacker are dropped.

Claims 15-16 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Kloth in view of U.S. Patent No. 6,389,532 (Gupta et al.). Gupta et al. disclose a method for using digital signatures to filter packets in a network. The method of Gupta includes discarding packets if the number of packets received from a source during a predetermined time period exceeds a rate limit.

Claim 15 is directed to a computer program product for generating filters based on analyzed network flows. The product generally comprises: code that separates data into different network flows and creates an aggregate network flow summary for one or more of the network flows; code that selects one or more network flows for analysis and analyzes the selected network flows by reviewing the aggregate network flow summaries; and code that detects potentially harmful network flows and automatically generates a filter to prevent packets corresponding to the detected potentially harmful network flows from passing through the network device.

Claim 15 has been amended to include code that creates an aggregate network flow summary for network flows and is submitted as patentable for the reasons discussed above with respect to claim 1.

Claims 16, 17, and 36, depending either directly or indirectly from claim 15, are submitted as patentable for the same reasons as claim 15.

Claims 18-20 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Kloth in view of Decasper et al. and U.S. Patent No. 6,453,345 (Trcka et al.). The Trcka et al. patent is directed to a network security and surveillance system which passively captures and monitors traffic on a network. The system continuously captures all data-link-level packets and routes this traffic to a high-capacity, non-volatile data recorder to generate a low-level archival recording. The storage device may be, for example, a high-speed magnetic tape drive. The recordings are used to reconstruct and evaluate network transactions to perform network analysis and restoration task, such as restoring lost data files. Applications are used to allow authorized users to analyze low-level traffic recordings to evaluate network events.

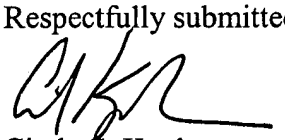
Applicant respectfully submits that claim 18 is not obvious in view of Kloth, Decasper et al., and Trcka et al. Trcka et al. is concerned with continuous recordings of raw data packets present on a network. The raw data is then used to gather network information and may be used off-line to allow users such as network managers to evaluate their network. As discussed above, Kloth is concerned with processing IP data using real-time data. Recorded raw data would not benefit data processing performed by Kloth. Hence, absent improper hindsight, there is no motivation existing in the art for combining the teaching of these references.

Accordingly, claim 18 is submitted as patentable over the prior art of record. Claims 19-21, depending directly from claim 18, are submitted as patentable for the same reasons as claim 18.

IV. Conclusion:

For the foregoing reasons, Applicant believes that all of the pending claims are in condition for allowance and should be passed to issue. If the Examiner feels that a telephone conference would in any way expedite the prosecution of the application, please do not hesitate to call the undersigned at (408) 446-8695.

Respectfully submitted,



Cindy S. Kaplan
Reg. No. 40,043

RITTER, LANG & KAPLAN LLP
12930 Saratoga Ave., Suite D1
Saratoga, CA 95070
Tel: 408-446-8690
Fax: 408-446-8691